Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
	)	PP Docket No. 92-234
Inquiry into Encryption Technology	)	
for Satellite Cable Programming	)	

NOTICE OF INQUIRY

Comments of Scientific-Atlanta

Scientific-Atlanta is a world leader in broadband communications systems, satellite-based communications networks and instrumentation for industrial, telecommunications and government applications.

The company is a recognized worldwide leader in the development and manufacture of systems used for the secure transmission of video and audio, in both analog and digital formats. Scientific-Atlanta is a leading supplier of subscriber systems to cable operators, with over six million cable converters installed throughout the U.S.

The company provides satellite encryption products to Primestar, a Ku-band DBS service. The IRDs incorporate the latest in advanced security techniques, including a secure microprocessor to prevent tampering with the decoder, advanced fourth generation security and "smart cards" for replaceable security. This security system has been tested and evaluated by independent security organizations which specialize in communications and computer security. No vulnerabilities have been found in this system.

Scientific-Atlanta is the leading supplier of satellite receivers to the cable industry. Scientific-Atlanta is familiar with the VCII technology as Scientific-Atlanta includes the VCII decoder module in many of these receivers.

In addition to providing equipment for the secure transmission of video, Scientific-Atlanta has extensive experience is developing subscriber authorization systems, similar to the one run by GIC referred to in the Notice of Inquiry. Scientific-Atlanta has developed national subscriber authorization systems for ICT, a digital audio service available over cable and satellite, and for Primestar.

In this Inquiry the Commission is examining relevant developments in encryption technology in order to explore the possibility that, with the introduction of new technologies, there is an alternative to the current de facto monopoly on encryption technology. Scientific-Atlanta concurs that this is a question which deserves investigation, and that viable technical and business approaches exist which can provide an alternative to the existing monopoly, both today and in the future. These alternatives should offer numerous economic benefits to consumers, particularly those who receive programming via satellite.

Our response will address those issues and concerns with which our company is most familiar and which are most directly related to "encryption technology". In our response we will reference the headings used by the Commission in their Inquiry.

Section I.3. Comments regarding historical description Scientific-Atlanta submits that the Commission's historical description in Section II is not totally complete.

Among several points which could be made, we note that even after the "free upgrade" is complete, consumers will own approximately 500,000 VCII+ modules which are not capable of accepting a "smart card" in the event of a future security upgrade. These modules would have to be completely swapped out (as were the VCII modules) in the event of an upgrade. Of these 500,000 modules, around 200,000 are covered by a limited "security warranty" which provides for a no-cost replacement unit. Another 300,000 units are not covered by any warranty and consumers would have to bear the cost of a future upgrade.

Section III. Competition in the provision of VC II Decoder Modules

The Commission asks a number of questions dealing with issues including:

- the impact of competition on pricing
- the impact of competition on the cost of a security upgrade
- viability and desirability of a non-GIC supplier of modules
- considerations of a programmer in determining whether to authorize non-GIC decoders
- how would competition affect the security of encrypted satellite signals

As in any marketplace, competition works to lower prices and increase the features offered to consumers. Competition in the satellite encryption market would have the same effect on modules and IRDs. By lowering module prices it could significantly reduce the cost to consumers of any swapout of existing VC II+ modules which are not equipped with renewable security. Competition would also give programmers more options in dealing with suppliers regarding an upgrade program by forcing manufacturers to compete on the price and availability of "smart cards".

As the Commission notes, security in the present analog video world consists of two elements:

1. The encryption algorithm by which the video and audio signals are coded. In the VC II system, the analog video is "soft-scrambled" using a technique which is not very secure. The strength of the VC II encryption is that the audio signal is digitized and encrypted.
2. The conditional access consists of successfully protecting the encryption keys and encryption algorithms stored in the decoder which authorize service. The pirate attacks on the VC II succeeded in breaking the physical security of the conditional access system.

As the Commission noted, there is value to consumers and programmers in having a common format in which all services can be received. This factor was the driving force behind the formation of the current de facto standard. In Section V. the Commission asks what encryption and conditional access technologies are available and/or already in use and how could they provide competition to the VCII. Before addressing this issue, certain parameters should be considered:

Any competition to the current de facto standard must operate within the practical technical and business boundaries of the present situation. These include the need to maintain interoperability within competing systems, both at the programmer and consumer level. In other words, competing systems/modules must both be able to receive all of the existing services and must not require complete overhaul of existing business systems of the programmers and packagers or major equipment upgrades by consumers.

Each video service today uses one satellite transponder. Satellite space is a scarce commodity, thus competing systems for encryption and conditional access must coexist within the same satellite signal.

Scientific-Atlanta believes that there are several existing approaches which could be implemented to provide competition in the current analog market. These are examined below:

1. Multiple licensees of current VCII+RS system
   The simplest and most direct method to encourage competition would be to allow multiple qualified manufacturers to design and produce decoders compatible with the current VCII+RS modules. GI would have to license its technology at a fair and reasonable rate, and would have to disclose enough technical information to allow manufacturers to develop their own implementation. Under this scenario, it would make sense to use the current authorization center to authorize all modules.

2. Use current video and audio encryption with a supplementary conditional access datastream
   Under this scenario GI would have to license its audio encryption technology and to provide the audio encryption keys. The competing manufacturer could easily decrypt the video without access to any GI technology. Competitors would develop their own conditional access (CA) systems. This CA data would be inserted into an unused portion of the VCII+ signal (e.g. the VBI).

   The competing manufacturer would have to develop an encoder and control computer to insert and manage the supplementary CA data stream. Programmers would have to install these to

interface with each existing VCII+ scrambler. A master conditional access computer is required to authorize and manage all of the decoders. The existing computer at the DBS center could be modified to do this, or a new CA computer could be developed by the manufacturer.

This new computer would have to interface with the business computers of the approximately 20 program packagers. This interface could be accomplished by modification of each of the 20 business computers, or via a relatively simple connection to the GI authorization center (in which data intended for the competing decoders is diverted to the second CA computer). This connection would require the cooperation of GI.

Overall, this approach is feasible from a technical viewpoint, but will require a significant investment in upfront development of computers and encoders and systems. The probability for success of this option is impacted by the level of cooperation from programmers and GI.

3. Use current video with a supplementary conditional access and audio datastream

   This approach is essentially the same as the second option except that a supplementary encrypted digital audio datastream is added to the existing satellite signal. Programmers would have to add an audio encoder/encryptor for each scrambled channel. The advantage of this approach is that it avoids the need to deal with GI regarding a license for their audio encryption technology.

   This approach is more costly to the manufacturer and consumer in that the hardware required to receive this additional audio channel adds cost. In addition, due to the limited bandwidth available in the satellite signal, it is likely that there would only be room for one competitor to send an additional audio channel.

As outlined above, several approaches are technically feasible for providing competition to VCII. Whether or not any of these is implemented, and which one is implemented, depends on business issues such as the level of cooperation from the programmers and GI, and the investment required vs. the perceived return.

The Commission asks about the viability and desirability of a non-GIC supplier of modules. There are likely only a very small number of firms with the technical and system expertise to carry out the approaches to competition outlined above. Programmers would consider the firms' technical prowess and ability to maintain security in considering whether to authorize non-GIC decoder modules. It has been reported in the press on numerous occasions that programmers, receiver manufacturers, dealers and consumers would welcome a non-GIC supplier.

Competition could have a positive effect on the security of encrypted signals by encouraging competing manufacturers to incorporate the most modern and reliable security techniques in their products at the lowest prices. Programmers would be able to choose the system/products they felt were most secure, and to penalize the manufacturer of less secure products (for instance by not authorizing their modules). Programmers would have to carefully evaluate the capabilities of manufacturers, and only select those qualified to design in and maintain the necessary security elements.

Section IV. Access to DBS Authorization Center

The Commission asks a number of questions about the DBS center. As noted earlier in this response, access to the DBS center is a critical issue in the development of a competitive product. The cost to duplicate not only the functionality but also the interfaces of the DBS center to the various program packagers represents a significant barrier to new entrants into the marketplace. Access to the DBS center, even on only a limited basis wherein communications protocols, etc., could be shared, would greatly assist in the development of a competitive product.

Section V. Other Technological Issues

The Commission notes that the world is moving towards the transmission of digital video and seeks comment on how this move may affect consumers and what technologies may be available to smooth the transition from analog to digital. It also asks about how other technologies can provide competition to VCII.

Digital video transmission offers several advantages over analog transmission, chiefly being that more signals can be squeezed into

the same bandwidth. Several programmers have plans in 1993 to launch new services using digital video, and have plans to move certain of the current analog programming to digital. This conversion of analog programming to digital will continue over time, but it is likely that analog transmission will still be used for many years.

These digital signals are primarily aimed at cable and SMATV headends which will deploy new digital IRDs to receive these signals. TVRO subscribers with their current IRDs and VCII+ modules will not be able to receive these digital signals. The conversion to digital is much easier for the commercial marketplace than for the TVRO market, because any one programming service may have only 500 to 25,000 affiliates, vs. the TVRO population at close to one million subscribers.

It appears that TVRO subscribers will be required to purchase a new satellite receiver and decoder module (design and technology yet to be determined) in order to receive these digital signals. This new IRD will be capable of receiving and decoding both the digital and the existing analog VCII signals. Because the new decoder must be able to decrypt the existing analog signals, and because the current DBS center will likely service the new digital/analog subscribers, the current de facto monopoly maintained by VCII will continue into the digital world.

Manufacturers who wish to offer decoder products capable of receiving both analog and digital signals will be forced to either

- build a separate digital module and purchase an analog module from GI (at a very high price) OR
- pursue one of the approaches outlined above for competition in the analog VCII marketplace. This would allow the manufacturer to have one decoder module which decodes both analog and digital signals (as GIC will be able to do).

In either case, any manufacturer wishing to serve this market will be at a significant disadvantage, if they are able to compete at all, to GIC.

<u>Interoperability considerations for digital video systems</u>

Scientific-Atlanta has invested a great deal of time in working with the cable and programming industries, both in the U.S. and around the world, in order to determine the key requirements for digital video

systems. We believe that interoperability is a critical element for future systems.

Interoperability can be defined loosely as the ability of products and equipment designed and manufactured by one company to operate interchangeably in a system with products and equipment designed and manufactured by another company. In a competitive market, challenges to interoperability arise when individual companies seek to gain a competitive edge by employing proprietary techniques that have resulted from their own investments in R&D. Also different market applications and market introduction schedules can complicate interoperability issues. Finally genuine difference of opinion exist on the impact of specific compression techniques on subjective evaluations of picture quality.

Pressures toward interoperability in the competitive market come from four sources:

1. Customers want to avoid sole source procurements.
2. Manufacturers can't afford development costs and high risk of being wrong in their choice of technology.
3. Programmers and consumers demand all programming in same format.
4. Regulators want standards.

There are two extremely important advantages of interoperability that sometimes are not emphasized as much as the four listed above. These advantages can be summarized as follows:

1. When the leading companies in an industry agree on an interoperable system, that system incorporates the best features and ideas from the research and development of those companies and the industry benefits from the best combination of leading technologies.

2. All techniques and approaches are carefully analyzed and scrutinized by multiple independent experts in the field and the true merit of any particular technique or technology can be differentiated from marketing hype.

At the heart of generating truly interoperable products and systems, are organizations like the EIA, ANSI, IEC and ISO. The EIA allows companies that compete vigorously in the marketplace to achieve technical consensus to arrive at voluntary industry standards in

critical areas required for interoperability. When organizations and industries beyond the EIA are critically involved, joint standards committees allow all affected parties to be represented in the standard making process.

All of us in the electronics industry, and particularly those of us in the generation, delivery, processing and display of information in the form of video, audio, data and text recognize that we compete in global markets. For that reason, it is increasingly important that we consider interoperability on a global scale rather than just on a domestic scale. Organizations such as the ISO, IEC, CCIR and CCITT provide the vehicle for establishing the requirements and standards for global interoperability.

In a digital world, video, audio, data and text will become increasingly interchangeable and interoperability needs to be considered not just on a domestic scale, but rather on a global scale. International standards and standards across industries will become more and more crucial.

The advent of digital video creates an opportunity to achieve an international standard that will eliminate the technical, operational and cost problems that have resulted from multiple analog standards such as NTSC, PAL and SECAM. One view of MPEG is that it is the digital compression international equivalent of the analog television standards: NTSC, PAL or SECAM. MPEG becomes the interoperable link for television in the digital domain from the studio through the transmission process to products in the consumer's home.

The need for a standard that provides interoperability is even more important now than when NTSC, PAL and SECAM were established because of the multiple delivery paths for television and the growing interface requirements with computers as well as consumer electronics. In the early 1950s when NTSC became a standard, television was primarily received by over-the-air broadcasts. Today, 60% of the homes in the U.S. receive their television via cable. About 75-80% of the homes have VCRs as a source of store and playback for television. MMDS, DBS and telephone companies are emerging as delivery mechanisms. Video disks and optical disks will become the device of choice for storage and playback. It would be foolish and risky for any one of the industries involved, including the back yard dish market, to launch a digital video compression service that did not consider the MPEG II standard. In fact, both TCI,

HBO and Viacom have announced that they will be using systems for digital video transmission which are compatible with MPEG II.

The levels of interoperability

Interoperability of the equipment for transmission and reception of television can be achieved at several levels. In today's analog television world, there are essentially only three levels of interoperability:

Level 1	Baseband Video and Audio
Level 2	RF Modulated Video and Audio
Level 3	Conditional Access/Security

The existing products/systems which deliver analog video today are compatible at levels 1 and 2, while it is in level 3 that they differ.

The advent of digital compression complicates and expands the concept of interoperability because of the need for error correction associated with modulation and the ability digital formats provide to multiplex multiple video and audio at variable data rates, along with other digital signals in the bandwidth of today's satellite, cable and broadcast channels.

For multichannel digital video compression transmission, we can define four levels of interoperability:

Level 1	Baseband digital video and audio for an individual television signal
Level 2	Multiplex and transport configuration and control
Level 3	Modulation and error correction
Level 4	Security and conditional access
	A. Encryption algorithm
	B. Conditional access data stream

Scientific-Atlanta's position on these levels of interoperability is as follows:

Level 1

Baseband video compatibility is being addressed by the MPEG II standard. Baseband audio is still being addressed in the international standards bodies, but a consensus should soon emerge. For interoperability between systems, all products should use these international standards.

Level 2

We have coined the term "Universal Transport Layer" to mean the data packet structure and associated control data that provides the mechanism to send multiple digital services at different data rates with security and addressable conditional access for each service. The significant features of the Universal Transport Layer include:

1. Standard Digital Sampling (CCIR 601)
2. Flexibility of data rates
3. Flexibility of data allocation among services
4. Flexibility of video and audio compression algorithms
5. Tailoring of error correction for ruggedness
6. Fast signal acquisition
7. Conditional access separated from services

With the Universal Transport Layer, each service (video, audio, text, computed data, telephony) can be thought of as an independent transmission pipe. The transmission within any one of the pipes is independent of the type of coding that is used for the digital service within the pipe. The data rates of the services within the pipes can be varied almost continuously over a wide range and the allocation of data to the individual pipes can be varied within the total multiplex range.

For interoperability between systems/products, a common transport layer and multiplex configuration should be adopted.

Level 3

It is essentially universally accepted that QPSK will be the modulation of choice for satellite transmission. The Commission and its process for digital HDTV will undoubtedly decide what modulation technique will be used for terrestrial broadcast. CableLabs is conducting analyses and making quantitative measurements comparing modulation alternatives for digital video in cable systems.

Level 4

The conditional access is independent of the transport layer and a separate data stream provides the addresses, tiering information and security keys required in a subscription conditional access system. For complete interoperability for paid subscription systems, the encryption algorithm for video, audio, text and data should be compatible for all equipment in the system.

It is possible to have a common and interoperable security encryption algorithm with a proprietary conditional access data stream that is unique to a specific supplier or to a specific system. In the interest of reducing the vulnerability of any transmission system to piracy, it is desirable for each supplier to have the option of a unique conditional access data stream.

Implications of adoption of digital video by the cable and programming industry on the TVRO industry

As was the case in analog video, the cable and programming industries adopted technology to suit their needs, which are the delivery of programming to cable headends and subsequent redistribution to subscribers. The TVRO market was not a target market but a byproduct created by the ability of consumers to receive these satellite signals directly. A similar situation is happening today as programmers adopt digital video, and the TVRO industry will attempt to develop products which allow consumers to receive these digital signals.

TCI, HBO and Viacom have all announced services they plan to offer via digital transmission. As the Commission noted in respect to the analog video marketplace, there is value to consumers and programmers in having a common format in which all services can be received. This factor was the driving force behind the formation of the current de facto standard in analog video.

As we move into the world of digital video, we face the same issues that existed when analog video first was encrypted, in that there appears to be a need for a common format for digital video. There is also a need to avoid the business arrangements which created the current uncompetitive situation in the analog marketplace. Scientific-Atlanta believes that the solution to these needs is in the adoption of an interoperable system. This includes the need for fair and reasonable cross-licensing arrangements to cover those elements of the system which are common. Such a system will ensure that the largest number of users have access to the most programming at the lowest prices.

The adoption of an interoperable system for the provision of digital video should be beneficial to much of the marketplace. However, even with the advent of digital video the TVRO market will still

operate in a hybrid analog/digital world for many years, and to the extent the analog encryption market remains uncompetitive, the TVRO market will continue to suffer from the problems which exist today.